**INFORMATION WARFARE CASE STUDY**

**IW 240**

**OPR:** Captain Gerard H. Eisert

**DESCRIPTION:** This lesson discusses how various pillars of Information Warfare can be used by our adversaries to influence our mission capability.

**METHODOLOGY:** Informal Lecture and Case Study/1 Hour

**COGNITIVE OBJECTIVE:** The objective of this case study is for each student to comprehend how IW can be used as a force multiplier by our adversaries to affect the warfighter's capability to wage war in the information age.

**SAMPLES OF BEHAVIOR:**

1. Discuss how political warfare affects warfighter's capability.
2. Discuss how economic warfare affects warfighter's capability.
3. Discuss how social warfare affects warfighter's capability.
4. Discuss how Information Warfare affects warfighter's capability.

**AFFECTIVE OBJECTIVE:** The objective of this case study is for each student to respond positively to the concept of how IW can be used as a force multiplier by our adversaries to affect the warfighter's capability to wage war in the information age**.**

**SAMPLES OF BEHAVIOR:**

1. Actively participates in case study how IW can be used as a force multiplier by our adversaries to affect the warfighter's capability to wage war in the information age.
2. Discuss how strategic decisions in the IW realm can affect units at the tactical level.
3. Offer real world experiences on the use of IW by our adversaries have affected their unit's readiness.

**REQUIRED READINGS:**

1. *"How We Lost the High-Tech War of 2007," Col Charles J. Dunlap, Jr. USAF, The Weekly Standard, January 29, 1996, Instructional Circular pages 240-H-1 through 240-H-8.*
2. *"Sometimes the Dragon Wins," Col Charles J. Dunlap, Jr. USAF, Instructional Circular pages 240-H-9 through 240-H-30.*

# HOW WE LOST THE HIGH-TECH WAR OF 2007

## A Warning from the Future

by Charles J. Dunlap, Jr.

*The following is the transcript of a secret address delivered by the Holy Leader to the Supreme War Council late in the year 2007.*

In the name of The One Above, I offer greetings to my fellow warriors! Today, with His grace, I speak of our great victory over our most evil enemy, America. A little more than 10 years ago experts thought that what became known as the Revolution in Military Affairs would leave developing nations like ours incapable of opposing a high-tech power like the United States. With the help of The One Above, we proved them wrong. They were guilty, as those who defy the sayings of the divine usually are, of idolatry--though in this case they did not worship graven images, but the silicon chip. As though a speck of sand could defeat the will of The One Above.

At the heart of the "revolution in military affairs" were the amazing new technologies that Americans believed "would make cyberwar and information war the distinguishing feature of future conflict," as one of their experts, Richard Szafranski, put it in 1995.

American thinking about the revolution in military affairs was based on grand visions of long-distance wars - push-button conflicts against cybernetically inferior foes. Once again, the Americans neglected to study history's many examples of supposedly out-matched combatants prevailing over better-equipped rivals. And they took it for granted that their potential adversaries would accept the American interpretation of this "revolution."

But America's most likely opponents were invariably unlike America and thus not beholden to the American interpretation. The late 20th and early 21st century saw the reemergence of what British historian John Keegan called "warrior" societies. Like us, they are "brought up to fight, think fighting honorable, and think killing in warfare glorious." A warrior in such societies, Keegan wrote, "prefers death to dishonor and kills without pity when he gets the chance." The Americans ignored a warning from one of their own, Maj. Ralph Peters, who wrote in 1994 that the "new warrior class already numbers in the millions." Peters wrote that:

*[America] will often face [warriors] who have acquired a taste for killing, who do not behave rationally according to our definition of rationality, who are capable of atrocities that challenge the descriptive powers of language, and who will sacrifice their own kind in order to survive.*

Too many Americans assumed that warrior societies like ours lacked the sophistication to integrate new technology into a war-making doctrine that could defeat the United States. They neglected those, like Donald E. Ryan, who cautioned that "even technologically backward societies have a nasty habit of devising strategies to offset [America's] high-tech superiority."

Moreover, that "superiority" was never as great as the Americans hoped. The cyberscience that fueled the "revolution" did not require the mature infrastructures needed to produce traditional war-fighting platforms like ships, planes, and tanks. With such platforms the First World's military power once dominated global affairs. Information technology changed all that, because its requirements were far less demanding: Small numbers of people working with commercially available computers could perform more than adequate high-tech research and development.

Furthermore, Americans increasingly relied upon commercial, off-the-shelf cybertechnology. We could acquire the same products on international markets - and often more quickly than the bureaucratic Americans, fettered as they were by complex contracting rules and regulations. Though the Americans claimed that information technology would allow them to get inside an enemy's "decision loop," the irony was that we repeatedly got inside their 'acquisition loop' and deployed newer systems before they finished buying already obsolescent ones. With the advent of off-the-shelf armaments, the American military no longer possessed a monopoly on the most advanced weaponry available.

Americans also underestimated the effect of rapidly declining cyber-costs - for, as George Gilder accurately predicted, in the year 2000 we could purchase silicon chips for $100 with as much power as the $320 million defense supercomputers of the early 1990s. The Americans discovered this when they sought to use information warfare to corrupt and destroy our command and control systems. The effort proved futile because many communications devices became so inexpensive and miniaturized that our armed forces could afford to make them ubiquitous and redundant. It was virtually impossible for cyber-assaults to negate them all. In the end, attacking these proliferating methods of communication typically made as much sense as using a laser- guided missile to disable the rifle of an individual soldier.

Worse yet for the Americans, advances in computer software eroded the demand for highly trained specialists to operate complex weapons. Easy-to-learn graphic displays allowed poorly educated soldiers to quickly master elaborate but user-friendly war-fighting machines, rather like a 15-year-old American figuring out how to dispense Coca-Cola at a fast-food restaurant by pressing the right pictograph. Praise The One Above, the microchip ended the educational and training advantage the American military had enjoyed.

Because the Americans believed their information technologies reduced the need for conventional combat forces, they disbanded such forces in favor of trendy "information" units. These were filled not with well-trained, physically fit combatants, but rather, as Szafranski put it, "mind-nimble (not necessarily literate), fingertip-quick youth" who tended to equate their success at video games with competency to engage in real war. Thank The One Above, the easy capture of a few of these self-styled "digital warriors" yielded a treasure trove of intelligence data.

We found we could contend with the light, supposedly high-tech combat units that completed most of America's remaining battle forces. Since we no longer had to concentrate our forces to oppose the now-defunct armored formations that dominated the First Gulf War, we took our cue from methods used by the North Vietnamese against the Americans and dispersed our army into small, mobile combat teams that combined only when required to strike a common objective. Not only did this make our troops harder to find, it also forced the Americans to expend their limited number of precision weapons on what were often tiny groups of soldiers.

In any event, we decided not to worry too much if we could not always match the high-tech equipment of the U.S. military. We consoled ourselves with the knowledge that reliance on cybersystems was not an unqualified virtue. The prescient Ryan noted that "technologically advanced, information-intensive military organizations are more vulnerable to information warfare simply because they are information dependent." Besides, our technical deficiencies inspired us to innovation - approaches overlooked by the gadgetry-obsessed Americans.

For example, we viewed the technology-spurred globalization of the news industry as a means of making war. By the mid-1990s, international news organizations using the latest electronic wizardry no longer had to depend on government help in war zones. Operational security became impossible as news groups launched information-gathering and communications satellites, monitored proliferating Internet transmissions, gave their reporters self-contained communications suites, and even flew their own unmanned aerial reconnaissance vehicles to transmit real-time views of battle areas.

This phenomenally valuable information was, of course, available to us. We had no need to build costly satellites or even pay spies; instead, we could rely on the free flow of data, because the Americans rarely achieved the necessary political consensus to interfere with these modern "news-gathering" techniques. Furthermore, whatever patriotic or legalistic pressure the Americans could bring to bear on their domestic news people was wholly ineffective against scoop-hungry foreign reporters.

In fact, the technology-empowered media made "information equality," not "information dominance," the key to the "revolution in military affairs." For example, when the U.S. tried their pathetic cyber-based psychological operations to mislead our people, the world press quickly exposed the American deceit.

We agreed with those, like George J. Stein, who said that information warfare "is fundamentally not about satellites, wires, and computers. It is about influencing human beings and the decisions they make." And we were confident we could influence the American public and its poll-sensitive decision-makers.

Studying the Vietnam conflict, we were heartened by the remarks of a former North Vietnamese commander, Bui Tin:

*Support for the war from our rear was completely secure while the American rear was vulnerable... The conscience of America was part of its war- making capability, and we were turning that power in our*

*favor. America lost because of its democracy; through dissent and protest it lost the ability to mobilize a will to win.*

Our strategy was to make warfare so psychologically costly that the Americans would lose their "will to win." To do so we freed ourselves from the decadent West's notions of legal and moral restraint. And why not? Their so-called "laws of wars" were conceived by the First World to keep our people oppressed. Furthermore, their "law" presented no deterrent because the West demonstrated over and over that it lacked the conviction to enforce it. No, my friends, The One Above called upon us to use every tactic to defeat the cyberscience that the Americans thought would make them so superior. We would rather be feared than respected.

With that in mind, we found that the radical changes in news gathering and reporting allowed us to develop a strategy to exploit America's growing fear of casualties. We carefully noted how this obsession enabled far weaker adversaries to defeat the so-called "superpower." The deaths of 18 American soldiers in Somalia - followed by the telecast of a U.S. soldier's body dragged through Mogadishu's streets - caused a public outcry that forced a humiliated America to forsake its policy objectives. Similarly, the specter of casualties was enough to delay intervention in Bosnia in the 1990s despite the occurrence of outright genocide. The exasperated columnist George Will wrote that the "West . . . almost preens about having become too exquisitely sensitive to use force against barbarism."

Thus, it became part of our strategy to capitalize on television's power to influence decisionmakers by aiming to wage war in the most brutish - and public - way. This strategy fit our warrior nation well. Countries such as ours, organized as they are around exceptionally powerful ethnic, religious, or cultural forces and frequently endowed with potent internal security forces, are much more resistant to vacillations in public opinion than are the diverse, pluralistic democracies of the West. Because our people truly believed in America's wickedness, it was not necessary to hide our ferocity. Rather, we used ruthless tactics openly to intimidate the American people and break their resolve.

The "revolution in military affairs" did not, therefore, make warfare less murderous; war never developed into the almost genteel electronic exchange that some foresaw. To the contrary, with our strategy it became more savage than ever - at least in the eyes of the many Americans who in previous conflicts had been spared the unedited, real-time "virtual" battlefield presence that the new communication nets allowed. Families at home could now watch and hear their loved ones die.

Such hideous experiences destroyed predictions of "non-lethal" conflicts made by over-enthusiastic cyberprophets. Those absurd forecasts, combined with the memory of a nearly casualty-free First Gulf War, caused many Americans to conclude erroneously that the occurrence of any casualties was irrefutable proof that a campaign was inherently flawed and should, therefore, be abandoned.

We expected that the U.S. would try to wage this supposedly "bloodless" war by assaulting us from afar with cyberarms. Only the soft, convenience-loving West would think that the loss of electrical power or phone service would stop us. Techno-offensives that cripple civilian systems do not deter us. After all, our people are accustomed to far worse.

To counteract the effectiveness of cyber-attacks on our military forces, we trained them to operate autonomously if normal communications were cut. We used runners, low-tech signaling devices, and even coded statements of our leaders, broadcast on international news programs, to coordinate actions until contact was restored. As a last resort, our forces struck preplanned targets, martyring themselves in the process when necessary. Our primary aim, after all, was simply to cause casualties among the Americans. We knew we would have that chance. The Americans eventually had to use troops to try to dislodge us because even in the 21st century, as Bevin Alexander put it in 1995, "victory comes from human beings moving into enemy territory and taking charge." Nothing else succeeds in conflicts waged against warriors of our zealotry. We anticipated, however, that the U.S. would first attempt to weaken us with its airpower.

Our analysis showed that we could not stop their high-tech aircraft from hitting anywhere in our country. To find a way to protect our key facilities, we once again examined history and recalled how Somali gunmen had effectively used their wives and children as human shields. We also remembered that after the uproar following the bombing of the Al Firdos bunker during the First Gulf War, when hundreds of Iraqi civilians died in an attack on what the Americans mistakenly believed to be a command center, very few strikes occurred against Baghdad. The Americans feared - rightly, we believe - that the spectacle of their pilots killing "innocent" civilians would be too much for their public (and world opinion) to bear.

Since our doctrine called upon us to present the Americans with moral conundrums that would complicate their efforts to attack us, we fully integrated our military infrastructure into civilian areas. We buried major command posts and logistics bases below schools, hospitals, apartment complexes, and even places of worship. Our most vital facilities were built underneath POW camps.

We saw how Serb forces back in the 1990s successfully countered NATO's sophisticated airpower by chaining U.N. hostages to targets. We also observed how rebel Chechens took 2,000 hostages at Budyonnovsk and cowed the Russians into meeting their demands. Accordingly, hostage-taking also became an important part of our "revolution in military affairs." In full view of the world media, we shackled captives to vital structures and openly bound them to tanks and military vehicles. We even put some on air transports and helicopters!

In order to create diplomatic pressure on the United States, we took lots of hostages from other nations, even neutrals. We used them to coerce their governments into allowing us access to essential international satellites and communications centers, while denying the same to the Americans. We also made a concerted effort to take hostages from militarily weak nations so that America would not gain valuable allies. Time and again our efforts earned a bonus: America--for political reasons--was obliged to accept new "allies" whose logistical requirements and marginal fighting ability made them more of a burden than a help.

We constantly looked for imaginative ways to turn our technological shortcomings into decisive strengths. With material and expertise gleaned from governments hostile to the U.S., as well as help from criminals in the former Soviet Union, we were able to assemble a handful of crude nuclear devices by 2006. But America's powerful information-technology weapons left us without a reliable way to deliver The Bomb. Their F-22 fighters, theater missile defenses, and ultra-modern hunter-killer submarines were systems we could not realistically overcome. Ultimately, however, we found a way to use our nuclear weapons against America.

Many of you have confused expressions on your faces. You are thinking: "It was the Americans, not we, who used nuclear weapons in the Great War." Yes, our Military City was destroyed by an atomic attack that killed 30,000 of our people. Sadly, it was the Will of The One Above. But my friends, it was not an American weapon that exploded. It was our own.

I will explain. In warrior cultures such as ours nothing is more glorious than dying in battle. For us and for many non-Western peoples, martyrdom and self-sacrifice are cultural totems more valued than self-preservation. Accordingly, we allowed the people of our Military City the honor of dying for our cause. It was the Will of The One Above.

Shortly before the start of the war, we deployed a nuclear device to the Military City hidden in an ambulance (protected from air attack by its red crosses). Next, we induced the Americans to strike by constructing a genuine biological warfare laboratory in the heart of the City - realizing, of course, that their state-of-the-art intelligence sensors would easily identify it.

Predictably, the Americans sent their stealthful F-117 bombers and cruise missiles against the laboratory. Several journalists reported the progress of the raid on live TV. Just as the Americans dropped their bombs, we secretly detonated our atomic weapon. The spectacular fireball vaporized everything for miles, all to the horror of a global broadcast audience numbering in the hundreds of millions.

The world reaction to what was thought to be an American first-use of nuclear weapons was universal condemnation. The Japanese were especially appalled. Not only did they cease contributing to the effort against us, they also began systematically to withdraw billions of dollars invested in American bonds. U.S. financial markets panicked, and the American economy fell into chaos. Other important members of the world community turned against America as well.

Of course, the United States vigorously claimed innocence. But few believed its government, even among the nation's own people. Clearly, Americans had grown so cynical of their government that they were quite willing to believe it capable of anything.

Political dissent soon burned at the fabric of American society, and we managed to inflame that controversy even more. We told the press that we would take reprisals against American POWs for the nuclear "attack." As you know, this was the first major war in which America deployed large numbers of female combat soldiers. To carry out our plan, our fighters captured a few dozen.

The Americans believed that their nation could endure the sight of women as POWs. Perhaps they were right. Whatever the case, America was shocked by what we did next: We used our infamous Boys Brigade

to rape the women, and then to amputate their limbs and burn their faces. Though we let them suffer terribly, we were careful not to kill them. We told the world that our women suffered much more in the atomic catastrophe.

The events surrounding the 50th anniversary of the destruction of Hiroshima taught us that the condemnations would be few. We saw how many people - including plenty of Americans - overlooked Japanese atrocities during World War II to castigate the American use of The Bomb to end the war. We likewise portrayed ourselves as nuclear "victims" and gained a surprising amount of sympathy despite our acts against the prisoners.

We then returned the POWs to the Americans - we said it was a "humanitarian" gesture. We converted the repatriation into what they called a "media circus." In no way did we try to hide what we did; to the contrary, we advertised it - using video clips on the Internet - as a warning of things to come.

However prepared the Americans though they were to see their daughters come back in body bags, they were not ready to see them returned home strapped to wheelchairs, horribly mutilated, and shrieking in agony.

Traumatized relatives frantically demanded the removal of their wives and daughters from the combat zone, and those demands were swiftly met. But by 2007, women had become so incorporated into the structure of the U.S. military that their sudden withdrawal wrecked the effectiveness of the deployed forces.

As successful as this strategy was, we still wanted to strike the American homeland. This was not easy. By the turn of the century, America had developed fairly sophisticated methodologies to protect their critical military and civilian computer systems from cyber-subversion. Of course, we hired the best hackers around the world to challenge the American safeguards. Although they enjoyed some success, this was really a diversion.

We knew that direct cyber-attack could not do the kind of damage necessary to defeat the United States. Adopting B.H. Liddell Hart's strategy of the indirect approach, however, led us to concentrate our efforts against America's soft underbelly, Mexico. The Mexican economy depended upon computers, but its machines were not as protected as those in the U.S.

Our hackers were able to disrupt and corrupt them on a massive scale. At the same time, we used modern document technologies to print billions in near-perfect counterfeit pesos to further sabotage the economy. Finally, our clandestine assistance re-ignited the simmering Zapatista revolt in Chiapas.

The synergistic effect of these schemes was devastating. The Mexican government collapsed and the economy disintegrated. Millions of refugees flooded the United States, prompting desperate calls for military assistance to control the influx. Angry Americans loudly objected to troops fighting thousands of miles away when a crisis existed quite literally in their own backyard. Our plan, thanks to The One Above, worked perfectly.

We developed additional methods of bringing the war home to America. Naturally, we used terror bombings, but we prudently avoided traditional targets. In the last 10 years industrialized countries have perfected security techniques that make attacks against defended facilities very difficult. So we chose a more exposed target: America's swelling population of politically influential elderly. We planted bombs in elder-care facilities, public parks, medical centers - anywhere we thought they would gather. Soon, frightened seniors joined the burgeoning antiwar movement.

Our search for other low-tech ways of attacking America drew us to environmental warfare. We waged it against U.S. agriculture because agriculture was virtually unprotected and within our means to strike. Our proxies spread destructive Mediterranean fruit flies throughout growing areas in California and Florida, and introduced various plant funguses and blights into Midwest grain crops. We also secretly inoculated farm animals with highly contagious diseases.

We used the indirect approach again by attacking other vulnerable targets outside the United States. For example, our agents set huge fires in equatorial rain forests, raising fears in ecologically conscious America that the world's oxygen supply would be jeopardized. From inside our own borders we attacked the ozone layer by releasing damaging chemicals into the atmosphere. Of course, we did not concern ourselves with the effects of these actions on our own people because our faith told us that The One Above would protect us.

We bragged about our responsibility for all these deeds, staggering Americans with our willingness to attack them in every conceivable way. By the grace of The One Above there was no method of warfare

that we failed to consider: We left AIDS-infected needles on bathing beaches and polluted America's coastlines by scuttling oil tankers we covertly hired. Americans could not enjoy a meal, relax on a beach, or even breathe the air without wondering if they were about to become victims of yet another of our assaults. Just as we destroyed their confidence in government, we destroyed their trust in nature.
You know the rest, my friends. Though we rarely defeated the Americans on the battlefield, we were able to inflict such punishment that they were soon pleading for peace at any price. With their economy in ruins, their borders compromised, their people demoralized, and civil unrest everywhere, they could not continue. We had broken their will! They had no choice but to leave us with the lands we conquered and the valuable resources they contain. Of the many mistakes the U.S. made in adapting to the "revolution in military affairs," several stand out: America too often assumed that the revolution would favor technologically advanced nations like herself. She failed to consider how enemies with values and philosophies utterly at odds with hers might conduct war in the information age. Despite what many technology-infatuated strategists thought in 1995, cyberscience cannot eliminate the vicious cruelty inherent in human conflict. We taught the Americans that no computer wages war with the exquisite finality of a simple bayonet thrust. Most critically, America failed to deal decisively with barbarism when confronted by it. Had she demonstrated the will to face her responsibilities as a superpower in the post-Cold War world, nations like ours might not have dared oppose her - we keenly understand brute force and its consequences. Now the Americans beg for our scraps. So desperate are they that they send their children here to be our servants. We control their future! That is the price of defeat! This, my friends, is the ultimate meaning of the Revolution in Military Affairs! Let us praise The One Above!

## SOMETIMES THE DRAGON WINS:

A Perspective on Information-Age Warfare by Colonel Charles J. Dunlap, Jr., USAF
The views and opinions expressed in this presentation are those of the author alone and do not necessarily represent those of the U.S. Government or any of its components.

**Introduction**
I want to take this opportunity to thank the sponsors of this conference for providing me the opportunity to share my views with such a distinguished audience of international experts.

At the outset I must caution you that I use the phrase "my views" literally. Everything that I say is my opinion alone and does not necessarily represent the views or opinions of the United States Government, the U.S. Department of Defense, or any of its components, including U.S. Strategic Command.

My presentation this afternoon will center on an article I wrote last January for the Weekly Standard entitled "How We Lost the High-Tech War of 2007: A Warning from the Future." In writing it, I was influenced by my experiences serving in Africa during our relief efforts in Somalia. I was struck by the resourcefulness, cleverness, and fierceness of the Somalis in confronting us. With that experience as a starting point, I theorized about the broader issue of what impact information-age technologies might have on the less-developed world, especially as the cost of extremely capable and easy-to-use information systems continues to fall. I wondered to what extent cheaper technology might affect the combat capability of societies we had considered too resource-poor to challenge us.

Those of you who may have read my article will realize that it is not a technical document. Rather, it is an imagined tale wherein the leader of a mythical non-Western nation delivers an "after action" report to his colleagues in his country's "Supreme War Council." In his speech, the unnamed chieftain explains how he engineered the defeat of the United States in a conflict set in the year 2007.

The scenario I set out is deliberately vague, but it does imply that this mythical nation has invaded a weak neighboring state. America, together with other members of the international community, endeavors to expel the aggressors.

What I tried to do is put myself in the position of a potential adversary some ten years in the future and postulate how war might be waged against a high-tech power. In setting the scene for my fictional war I made a number of assumptions:

a) That Western nations, and particularly the United States, would develop and deploy sophisticated information-based weaponry (e.g., F-22 fighters), and would organize their forces and develop doctrine accordingly.

b) That these same nations would develop and deploy information-based methodologies that could defend their most vital civilian and military facilities not only from hackers and other forms of cyberassault, but also from Oklahoma City-style physical attacks.

Many of you may properly think that such assumptions are overly optimistic. Nevertheless, what I wanted to do is to hypothesize a "best case" scenario for the United States and the West.

Against this background my fictional enemy nevertheless masterminded the defeat of the United States by waging not limited war, but a new kind of conflict that I call "neo-absolutist war." This is a vicious form of confrontation that extends across the spectrum of warfare. It differs from more traditional "total war" by, among other things, the propensity of the aggressor to focus on shattering the will of an opponent by employing brutality openly and unapologetically against combatants and noncombatants alike. In a sense,

such warfare has existed throughout the history of man, but information-age technology modernizes it (hence the term "neo") and vastly expands its potential.

In order to explain the theories that High-Tech War of 2007 meant to illustrate, I've extracted a number of propositions that I'd like to discuss.

**Proposition #1:** Our most likely future adversaries will be unlike ourselves.

The adversary I invented for High-Tech War of 2007 is not a First World nation and perhaps not a nation-state in the traditional sense at all. Instead, it is more a grouping of peoples who are profoundly unlike ourselves in several critical respects. My analysis causes me to disagree with those - including some information-warfare gurus - who too often seem to assume that our future opponents will be Westernized, technology-dependent societies whose armed forces are built more or less along the same lines as those of the U.S. Likewise, I believe that many information-warfare enthusiasts mistakenly suppose that our future opponents will have cultural mores and values similar enough to ours so that a "rational" (in a Western sense) cost-benefit analysis would drive decisions of peace and war.

I do not, of course, entirely discount any possibility. Given the history of the twentieth century, I guess that it's theoretically possible that a high-tech Western European nation might wage war against the U.S. in the future. Furthermore, I recognize that we in the West are finding groups of rather bizarre extremists who might someday pose more than the mere law enforcement threat that they do today. But I still think the much more likely scenario is what Samuel Huntington called in his 1993 Foreign Affairs article of the same name, a "clash of civilizations."

What would be the nature of such civilizations with whom we might clash? In a fascinating piece in the summer 1994 issue of Parameters, Ralph Peters, then a U.S. Army major, described what he called the rise of "The New Warrior Class," a multitude which he contends "already numbers in the millions." Peters says that in the future:

[America] will face [warriors] who have acquired a taste for killing, who do not behave rationally according to our definition of rationality, who are capable of atrocities that challenge the descriptive powers of language, and who will sacrifice their own kind in order to survive.

In a similar vein, eminent British military historian John Keegan maintains that we are seeing the re-emergence of not just a warrior class, but warrior peoples who are psychologically distinct from the West. These are societies, he says, where the young are "brought up to fight, think fighting honorable and think killing in warfare glorious." A warrior in such societies, Keegan has written, "prefers death to dishonor and kills without pity when he gets the chance."

A civilization so composed, perhaps organized around some powerful social or cultural force, will be a most dangerous foe because of the uncompromising zealotry and ferocity with which it can wage war. In my scenario, the aggressor nation's motivating psychological force is an unspecified religion that completely dominates its culture. I might add that the driving force could have just as easily been an ethnic identification, political ideology, or even some kind of as yet unknown cult.

If one is looking for a prototype of the kind of adversary and type of conflict that I foresee, I would suggest studying the war in Chechnya. Despite the application of tremendous military power, savage fighting persists. I submit that a lesson of that conflict, and one that I'll talk more about later, is that such peoples are hardly the type to capitulate solely as a result of the "bloodless" information warfare techniques touted by so many as the future of war following the purported "revolution in military affairs."

These warrior societies (or "streetfighter" nations as one commentator aptly described them) actually enjoy certain warfighting advantages over the U.S. and the West. Their populations are usually much more

disciplined, casualty-tolerant, and able to endure deprivation better than we are. Their troops are unfazed by orthodox calculations of what is militarily "doable," and quite often have much more austere logistical and support requirements.

For most of the nineteenth and twentieth century, however, these warrior societies and streetfighter nations infrequently succeeded - in a purely military sense - against the technologically superior forces of the West, especially when the Western power put its full resources into the effort. Indeed, a common critique of my article is that no adversary like the one I invented could possibly conduct the global military and paramilitary operations necessary to achieve the victory I describe. However, I assert that new developments in cyberscience have the potential to prove my detractors wrong.

**Proposition #2:** Information technology will facilitate and hasten the consolidation of potential opponents, including warrior societies.

I believe that new, simplified, but enormously effective methods of communication will allow the consolidation of national and transnational warrior societies (as well as radical elements of streetfighter nations) to a degree hardly dreamt of today. Specialized satellite television networks, comsats, Internet gateways, faxes, cell phones, and all the other attributes of the global communications revolution may enable the formation of "cybertribes." These could unite what now might be a diaspora of like-minded peoples hostile to U.S. interests. We already know, for instance, that neo-nazi groups use the Internet to maintain contact with each other.

Enhanced communications can also be a catalyst that releases potent but presently inchoate psychological energy. That venting can produce violent results: one observer insists, for example, that the Milosevic regime "fanned the fires of pan-Serbism by taking over the national television system and using it to magnify semi-dormant hatreds."

Where once the word "communications" conjured up expensive networks of telephone lines, microwave towers, repeater stations and so forth, a defining mark of the information age is the radical decline in the cost of all forms of communications. New hardware such as direct broadcast satellites eliminates the need for expensive cable or fiber-optic distribution systems while making it possible to reach audiences numbering into the billions. A similar result is produced by the growing use of cellular phones. I once visited the Khyber Pass which, as you know, is in a desolate region of Pakistan near the Afghanistan border. To my great surprise I saw people who were living much as Rudyard Kipling must have found them, but who were, nevertheless, using cellular phones to maintain communications, often with the help of satellites.

Please note, however, that in the future it may not even be necessary for a less-developed nation to spend the huge sums necessary to launch satellites. The L.A. Times reported last month that the U.S. Marines were experimenting with communication "satellites" that are actually held aloft by high-altitude balloons as a less costly alternative to space-based systems. Obviously, a potential adversary could do likewise.

I am convinced that the employment of new and increasingly inexpensive means of communications can tremendously influence and mobilize significant populations against U.S. and Western interests. The leadership of the warrior "cybertribes" can use cheap communications to not only unite their followers, but also to exercise effective command and control over groups that might be widely separated yet whose aggregate capabilities create genuine military concerns.

Along this line I should note that a phenomena of warrior societies and extremist streetfighter nations is that they tend to produce charismatic leaders. Modern communications systems will enable telegenic leaders to leverage their personal "aura" to reach huge numbers of peoples. Even wholly illiterate people will be able to see and hear their leader via "telepresence." What's more is that coming holographic imagery will project the leader's charisma in an enormously convincing way and do so for audiences at

multiple locations. Perhaps more importantly, a variety of emerging information and communication technologies will also leverage the streetfighter nation's military capabilities.

**Proposition #3:** Most analysts dangerously underestimate how significantly emerging technologies will empower warrior peoples.

As I mentioned, a common critique of my article is that no such "warrior society" could ever carry out the sort of world-wide attacks that happen in the scenario. Such attitudes dangerously underrate potential enemies, and reflect an arrogance that has had unfortunate consequences for the U.S. and the West throughout history. In conflicts ranging from Vietnam to Somalia to the Balkans, we have repeatedly seen how crafty opponents can offset high-tech hubris. Frankly, I think my critics misread the true implications of the information revolution on military affairs.

One key implication is that our potential adversaries will be technology-enfranchised in ways which will obviate many of the advantages First World militaries enjoy today. The U.S. and the West seem to believe that they can safely downsize their forces so long as they maintain relatively small numbers of well-educated troops supplied with high-tech equipment. But I question how much longer we can expect to maintain a monopoly on the world's best trained troops. Realistic new combat simulators and self-paced computerized teaching technologies will make sophisticated training available to the masses in the less-developed world. Furthermore, this kind of technology does not depend upon the physical presence of foreign military trainers who might otherwise be able to influence and moderate warrior societies' actions.

In any event, I'm not at all sure how much technical training the average combatant will need in the future - my guess is that most will need very little. My article predicts that extremely user-friendly software will empower poorly-trained or even illiterate fighters to operate what is today considered complicated weaponry. Furthermore, some adversaries may abandon whole classes of weapons that require highly-trained operators (e.g., manned fighter aircraft) in favor of fully-automated, easy-to-use systems (e.g., anti-air missiles).

With the help of artificial intelligence systems incorporated into personal information devices, raw but determined conscripts might be able to use complex weapons in a strategically and tactically effective manner. The wisdom of the West Points, the Sandhursts, and the St. Cyr's of the world could be available - in the local language - to anyone who can wear a headset and push an "on" button. A step in this direction already exists in the form of what a company called Intervision calls the "computer-on-a-hip."

Because new technology can implant "expertise" into a military organization in so many ways, it may not be necessary to educate the force as a whole. I disagree, therefore, with those strategists who contend that success in future conflicts will depend upon the technical knowledge of individual soldiers. By using technology to replace the intellectual achievement that could previously be obtained only through laborious and time-consuming courses of study, the combatants on future battlefields will become much more equal than has historically been the case. Moreover, given the innate martial qualities of warrior societies, the diminishing importance of the educational credentials cannot favor today's high-tech nations.

Besides eroding the training and education advantage that the U.S. and the West are counting upon to maintain a military edge, I also believe that technology itself will be much more "level" on future battlefields than most people think. This coming parity can be largely ascribed to the fundamental difference in what Alvin and Heidi Toffler would call Second and Third Wave weaponry. "Second Wave" weaponry are the planes, tanks, and ships produced by industrialized countries. Nations without sufficient heavy industry to allow at least some degree of weapons' autarky had little hope of prevailing militarily in all-out struggles against countries so equipped.

Likewise, for most of the twentieth century, the invention of revolutionary new weaponry usually occurred in those nations able to sustain a rather specialized and militarily-unique research and development base. Again, in large measure, this was the industrialized West and, accordingly, the West could monopolize and control the creation and production of the most advanced armaments.

That, in my opinion, will not be the case much longer. The key to "Third Wave" warfare does not lie in producing traditional weapons platforms; rather, if the experts are to be believed, the critical element will be the new information technologies that are largely computer-sourced. For this reason I do not believe that tomorrow's information-based weaponry will be produced by another resource-intensive "Manhattan Project" or "Skunk Works." Obviously, it does not take a huge dedication of assets to turn out, for example, a piece of devastatingly effective software weaponry. Low-cost personal computers available in retail stores worldwide will more than suffice.

But a more fundamental reason the U.S. and the West will not have the high-tech advantage that they now possess is the simple fact that there are too many commercial applications of the new information technologies for the defense establishment of the United States or any other country to monopolize and control them. Businesses all over the globe are racing to invent new information-oriented software and hardware products. Accordingly, our future opponents (without investing anything in an indigenous R & D infrastructure) can leverage the whole world's research and development capacity as it looks for information technologies that have possible military uses.

There are additional reasons that the most up-to-date technology will be readily available to our potential opponents. Of course, producing computers is a much less taxing enterprise than building aircraft carriers so there will be far more sources, perhaps even the streetfighter/warrior nation itself. After all, the manufacture of some systems may favor countries - unlike the United States and those in Western Europe - with low-cost labor pools. In addition, notwithstanding the potential military applications of information technologies, third-party financing and economic assistance is much more likely to be available to a less-developed nation for this kind of venture than for a traditional arms industry. The inherent versatility of cyberscience means that a country can build an information infrastructure with military capabilities while simultaneously serving the needs of economic development and, incidentally, not necessarily arousing the world's suspicions. Our potential adversaries will not have to choose between "guns" and "butter" in building information-age warfighting capabilities.

Yet another reason that the battlefield will become more technologically "level" lies in the growing dependence of the U.S. and other armed forces on commercial-off-the-shelf or "COTS" technology. Plainly, this means that we have to expect that sooner or later our enemies can make similar purchases in the retail market. Like the decline in communication costs, the astonishing reduction in the price of computer power brings extraordinarily versatile systems within the range of even the poorest potential foes. Because of the ready availability of cyber-technologies and the continuing decline in costs, I contend that the era when the First World would produce and control the latest weapons is over - at least to the extent that information technology is the linchpin to the most sought after arms.

Furthermore, non-democratic opponents may well have another significant advantage over us. Specifically, their acquisition policies are not necessarily as fettered by Byzantine rules and regulations as are ours. We all know that information technology can become outmoded in a matter of months, and that's much too fast for our current procurement process to react very well. Thus, a totalitarian regime may well be able to get inside our 'acquisition loop' and procure and field advanced information-based weaponry before we can do so. In short, I am not confident that our existing contracting laws are dynamic enough to accommodate the information-age's environment of rapid technological change.

**Proposition # 4:** The age of mass warfare may not be over!

Incidentally, should my predictions on these points prove valid then, contrary to the forecasts of most experts, the era of mass warfare might not be over. As I've indicated, most First World militaries - including ours - are counting upon an advantage in high-tech weaponry and superior training to allow dramatic downsizing of forces. If, as discussed, our adversaries will have much the same technology as we have, and information technology can neutralize the technical expertise and training that gives First World forces so much of an advantage today, then the difference between victory and defeat might well revert to a question of the sheer numbers of combatants deployed. A future Napoleon might rightly echo the words of the original: "Victory goes to the big battalions."

In my estimation those in the U.S. who think that the Vietnam-era draft protests are little more than historical curiosities may be in for a shock. In the future we could find it necessary to conscript huge numbers of people to battle civilizations willing to place millions of technology-empowered citizens under arms. Even if the fashionable view prevails, i.e., that future armies will be populated by highly-educated cybersoldiers, I am not so sure that an all-volunteer force will be able to attract enough such specialists in the coming years that conscription can be permanently ruled out. Media reports of anti-draft demonstrations may again fill our television screens.

**Proposition #5:** The impact of information-age technology on the global media will be the most immediate and most powerful influence on information-age warfare.

In my opinion, the most immediate and powerful impact on future conflicts will be the ongoing media revolution occasioned by information-age technology. Parenthetically, it amazes me how little discussion there is about this in the reams of literature concerning the alleged "revolution in military affairs." What discussion exists is, in my view, incredibly naive and underdeveloped.

We already know that the media can project powerful images. What is new is the explosive growth in the media's ability to find and report these images from areas of armed conflict. Historically, governments with a mind to do so have been able to exercise considerable control as to reporters' access to war zones as well as the dispatch of stories from battlefields. The press was often forced to depend upon the benevolence of the armed forces for transportation and communication in combat theaters.

That will seldom be the case in the future. As I predict in my article, news organizations will own surveillance satellites and self-contained communication systems that will allow them to function almost totally autonomously. Indeed, one firm, Aerobureau of McLean, Virginia, run by Chuck de Caro, already can deploy a self-sustaining flying newsroom. The airplane is equipped not only with multiple video, audio, and data links, but also gyro-stabilized cameras, side and forward-looking radars and, believe it or not, its own pair of camera-equipped remotely piloted vehicles. In addition to being able to land on short unimproved runways, the aircraft can also dispatch satellite uplink-equipped reporters by parachute! Clearly, the media will be physically able to report the news, "live from the battlefield," totally independent of military support or, even more importantly, the military's permission.

While we might be able to prevail upon the ethics or patriotism of individual correspondents who are our own nationals, the growing globalization of the news will always leave foreign journalists willing to report and broadcast such intensely newsworthy events as armed conflicts, especially those involving U.S. or other First World forces. I am convinced that information technologies will empower the media to such a degree that virtually no observable detail of any consequence will escape their view. Furthermore, huge interconnected databases will add tremendously to their news sources. Advanced software will enable them to "fuse" the raw inputs into useful, real-time or near real-time reportage. Such developments, in my opinion, will profoundly affect the conduct of future war.

The media revolution is but another example of how the information age will diminish the First World militaries' current superiority. The press will become the "poor man's" intelligence service and this will help warrior societies and streetfighter nations to wage war "on the cheap." With immense quantities of

information available from global news groups, what need will there be for our future enemies to spend enormous amounts of money building Western-style intelligence infrastructures?

None of this should really surprise us. We already see decisionmakers of many nations relying upon information from media sources like CNN. Some might say that if the media serves as a de facto intelligence service for a hostile force, then they should be treated accordingly. I doubt, however, that Western democracies can muster the political will to forcefully block reporters' activities, especially those of the non-belligerent third-countries.

The media revolution will have another important effect on military operations: the increasing obsolescence of operational security (along with deception and psyops) as useful military concepts. The rise of aggressive, technology-infused global news organizations will fill the air with colossal amounts of data. Every military move, or seeming military move, will be scrutinized and analyzed by the press and the expert consultants they hire. In that context few military courses of action can remain concealed for very long.

I might add that it is not only the media that is responsible for this evolution. The proliferating numbers of personal cell phones, e-mail capable laptop computers, fax machines, and so forth that troops themselves carry with them will also contribute to the avalanche of information that will be available about military operations. I think that commanders will find these devices near impossible to monitor and censor. While our adversaries will have a similar problem, I think it will be more pronounced for the militaries of Western-style democracies because of the open nature of our societies.

Indeed, we are already experiencing an inkling of what's coming. I invite your attention to a recent report that 90% of Israeli recruits arriving for service brought along their own personal cellular phones. Some used them to call their parents and others to complain about various aspects of their military duties. As Newsweek predicted over five years ago, "if soldiers can phone mom or the local newspaper from the middle of the battlefield, what are the implications for maintaining military discipline or secrecy?" I think the obvious answer is that both will suffer.

**Proposition #6:** The technology-empowered media and the proliferation of personal information/communication devices will have the effect of limiting the practical ability of casualty-adverse democracies to engage in combat for much more than thirty days.

I maintain that the synergistic effect of the media revolution combined with a proliferation of personal information devices will make it politically unfeasible for most democracies to wage intense combat operations for much more than a month or so. During the Gulf War we saw how gruesome photos of the so-called "highway of death" undermined support for continuing the war - and those were pictures of the destruction of a brutal enemy invaders. What should we expect when the bodies are those of our friends and relatives?

In the future, the type of "real-time" reportage of death and mutilation of our own soldiers that the new technology makes possible will likely create unsolvable political problems. Tomorrow's communication capabilities may allow commercial news services to furnish soldiers' families with customized coverage of their loved one's unit, and perhaps even of specific individuals. This kind of coverage supplementing personal communications from the troops' own information/data devices will enable the soldiers' families to establish a "virtual presence" with them on the battlefield. When such "telepresence" begins to communicate the horrific shrieks and terrifying sights of death and mutilation as it happens to a loved one in combat, the political pressure to terminate hostilities at almost any price may become inexorable.

To accommodate this approaching reality, I think that the U.S. and other Western democracies may need to retain larger standing forces than are presently contemplated. We must be able to react swiftly to fight time-sensitive "come as you are" wars. Because there will only be a short period before the enhanced

communication of the horrors of war makes continuing simply not politically viable, there will not be enough time, for example, to prepare and deploy those reserves who require refresher training prior to combat. Rethinking the size and composition of reserve forces may, therefore, be in order. Similarly, if political demands dictate that fighting must be brief, then sustainment and reconstitution may be less important than many militaries think. In short, if a military solution cannot be achieved quickly, political exigencies may make it not achievable at all, notwithstanding the gravity of the interest at stake.

Planners for information-age conflicts ought to consider, therefore, training and equipping forces for extremely intense, hyper- or "blitzkrieg" style warfare. Regrettably, pressure for quick resolutions may compel military commanders to forego time-consuming tactics even though they might limit casualties on all sides in the long run. Once fighting has begun, I just don't think that the public will have the stomach or patience for methodical approaches even if they promise less bloodshed over time. Accordingly, it will be imperative to develop stratagems that maximize the application of combat power before public support and political will evaporate.

**Proposition #7:** Seeking "information dominance on tomorrow's battlefield is unrealistic and quixotic; instead, the U.S. should focus on developing doctrine and strategies for operating in an environment of "information equality" or "information transparency."

Among the stratagems, however, that should not be counted upon for achieving rapid military success is the notion of gaining "information dominance." For all the reasons I've mentioned - the likely technological parity of future belligerents, the stupendous multiplication of personal information devices and, most importantly, the explosive growth of the technology-empowered media - it will be nearly impossible for any belligerent to "dominate" the information dimension. What we should do now is not chase an unrealistic and quixotic strategy of "information dominance," but rather we ought to be thinking about how forces will fight in an environment of information equality or, perhaps more realistically, a totally transparent information environment, i.e., where each side knows everything about the other.

As already described, the nature of the information age will likely find ourselves with equipment at best equivalent to that of our enemy, and very possibly inferior. Even if we were able to deploy somewhat superior devices, I still think that achieving true "dominance" in anything more than a transient, tactical sense will be frustrated by our inability to degrade enemy systems. Information technology, and particularly communication systems, will become too inexpensive, too compact and, consequently, too redundant for military or cyber-action to neutralize all of them.

I can foresee a time when the communication capabilities that today require entire units will be found in the personal information devices I've mentioned. There will no longer be any key communication "nodes" upon which to focus an attack - ultramodern information technologies will turn individual soldiers into self-contained communication centers. In fact, the L.A. Times article I referred to previously reports that the Marines are experimenting with small three-man groups linked to units by computers as a substitute for personnel-heavy command structures. To take out all of the new style C3I "nodes" will mean, literally, destroying every combatant on the battlefield. And, when confronting warrior peoples and streetfighter nations, such bloody business may be exactly what information-age warfare requires.

**Proposition #8:** Information-age warfare will not become an "almost bloodless" electronic exchange that some predict; rather, it will be as savage, and likely more savage than ever.

One of the principal reasons I wrote the High-Tech War of 2007 was to attack what is becoming conventional wisdom in the United States and many Western nations: the idea that information technologies will allow wars to be waged virtually bloodlessly. In a scenario depicted in Time magazine last summer, a U.S. Army officer conjured up a future crisis where someone like himself ensconced at a computer terminal in the United States could derail a potential aggressor "without firing a shot." He visualized the foe's phone system brought down by a computer virus, logic bombs ravaging the

transportation network, false orders confusing the adversary's military, television broadcasts jammed with propaganda messages, and the enemy leader's bank account electronically zeroed out. All of this is expected to cause an opponent to capitulate without fighting.

I don't really know if what he implies is technologically possible. I do think, however, that he is failing to anticipate a point I've tried to emphasize: that future information technology may become so inexpensive that aggressively-minded nations - even relatively impoverished ones - will be able to afford redundancies that will make it difficult or impossible to accomplish what he suggests. Consider that the Internet, access to which only requires an inexpensive computer, originated in a system meant to survive a nuclear attack by exploiting redundancies in modern communication processes. Surely critical communications and information technologies based on this or similar systems will be very difficult to defeat.

Once again it seems that the ability of foes to devise low-tech ways to circumvent high-tech capabilities is being underestimated. Should we not anticipate that our future adversaries will plan work-arounds for precisely this kind of cyberassault? But even assuming the colonel's plan is technologically feasible, and assuming the profound legal, ethical, and policy issues that his storyline raises can be resolved, I still maintain that it reflects a fundamental misunderstanding as to the character and temperament of our most likely future opponents. Warrior societies and streetfighter nations are just not as vulnerable to technology loss as is the U.S. and the industrialized West.

To me the Army colonel's scheme also mistakenly takes for granted that future foes would plan to fight us in the same high-tech way as we would, and that they would engage in the kind of cost-benefit approach to conflict that the U.S. and the West do. It may be that we in the West in the late twentieth century might be ready to abandon a military effort if our phone and electrical systems were disrupted, or if our bank accounts were emptied. But it is a peculiarly Western notion to presume that every enemy in a future conflict would back down for like reasons. I would not count on such discomfiture deterring a warrior society acting in pursuit of a powerful cultural imperative and under the spell of a charismatic leader.

In any event, I doubt that a warrior society or streetfighter nation would try to defeat us by assaulting our domestic information infrastructure. I believe they would conclude - as the potentate in my article does - that to do so is too difficult for a less-developed nation with limited resources. I anticipate that they would determine that the 'center of gravity' in conflicts with First World democracies is not the information infrastructure per se, but the will of the people in a Clausewitzean sense. They will concentrate not so much on destroying our things, but on smashing our spirit. In doing so, they may well decide that preserving our information infrastructure actually facilitates their strategy - it helps them to graphically communicate their willingness to do anything for victory, however despicable.

Streetfighter nations like the one in my scenario will feel no compunction about waging war - particularly against the West - completely outside the norms of international law. Indeed, in my story their strategy is to deliberately wage war in a most inhumane and public way possible as a means of intimidating us and undermining our will to win. I think emerging information technologies will enable them to do that in quite innovative ways. This further explains what I mean by neo-absolutist war: Total war ruthlessly waged by unconstrained enemies enfranchised by technology.

That said, I should note that while a few of our future enemies will no doubt be sociopathic, I do not mean to necessarily suggest that their whole society would be similarly affected . I think that some groups may be able to form a moral, political, or cultural construct that leaves those outside of it unworthy of humane treatment. Aiding and abetting such a weltanschauung might be real or perceived affronts occasioned by U.S. or the West's actions, perhaps not even of recent origin. What I am saying is that adversaries' populations might somehow be able to rationalize abominable behavior in a war with a high-tech power.

Accordingly, I believe that a future opponent will not hesitate to use brutality to exploit the growing aversion to casualties that more and more shapes the political and military decisions of the U.S. and other First World countries. Consistent with neo-absolutist war, atrocities will be brazenly displayed, not

hidden. Our enemies will seek to manipulate us through barbarism, and enhanced information age technologies will help them do just that.

Why would they choose this strategy? For the simple reason that they might believe, rightly or wrongly, that it has worked in the past. To explain what I mean I invite your attention to another criticism of my essay: an adversary who conducted himself as the one in my story would so incite the U.S. that America would never abandon its military effort until the enemy was fully prostrate. I hope that would be true, but I wonder. Did that occur when Somalis dragged the body of a U.S. soldier through the streets of Mogadishu? No, it did not; there was no public demand to crush the perpetrators.

Although there were many complex reasons for the subsequent U.S. withdrawal, I worry that our future enemies might conclude that the atrocious behavior the Somalis displayed helped undermine U.S. public support for the whole operation. If that is so, then the perceived failure to make those responsible pay a terrible price for such barbarism might encourage even greater viciousness in future information-age conflicts.

I fear that one target of their strategy will be prisoners of war. POWs became an important bargaining chip for the Communists during the Vietnam War and they were often used for propaganda purposes. In my scenario, female POWs were particularly victimized by an enemy hoping to capitalize on our domestic debate concerning the extent to which women should be involved in combat. That victimization was not done in secret; rather, the enemy employed modern communications to broadcast - live - the torture of the POWs to their families at home. Clearly, this was designed to demoralize us and erode our will - a classic example of neo-absolutist war.

A few might wonder who could commit such terrible crimes. Apart from the fact that the twentieth century has witnessed more than its share of such deeds, last August Newsweek magazine reported a disturbing trend: several Third World countries are recruiting young teenagers and even pre-teens into their armies. Among the reasons for doing so, Newsweek concluded, was that "boys will do things grown men can't stomach." A UNICEF worker observed that "kids make more brutal fighters because they haven't developed a sense of judgment". Along this line you may recall that most of the Somalis mugging for the camera with the body of the U.S. soldier were youths in this age group. Because a basic tenet of neo-absolutist war is brutality, we might expect that young fighters will become a staple of many of our adversaries' soldiery.

The inexpensive but powerful communication capabilities we've discussed will allow a future opponent to off-set other aspects of our current military superiority, especially when aided by willingness to ignore fundamental precepts of humanity and the law of war. For instance, our opponents will be able to maintain command and control while at the same time dispersing their forces in such a way as to be extremely difficult to find and destroy. I foresee "virtual armies" composed of small numbers of people, even individuals, remaining widely dispersed until immediately prior to an assault, if then. In carrying out this tactic, I believe that our enemies will present ethical quandaries for First World nations by purposely dispersing themselves among noncombatant civilians. Every attempt to strike them will risk noncombatant casualties.

Some might believe that information-age precision-guided munitions are the solution. But I think that underestimates the ingenuity of an enemy prepared to wage neo-absolutist war. In my story, for instance, the adversary counters the U.S.'s advantage in high-tech airpower and precision-guided munitions by building VIP shelters, supply depots, and other vital facilities beneath hospitals, apartment houses, churches, and even POW camps. The clear aim of the enemy was to create the same kind of dilemma as did the bombing of the Al Firdos bunker during the Gulf War. You may remember that what was thought to be a command bunker apparently housed Iraqi civilians, many of whom were killed in a strike by the precision munitions delivered by F-117 stealth bombers. Because of the political furor that ensued, attacks on Baghdad were sharply curtailed.

In a way, information age technology and its success in the Gulf War have produced a problem for the U.S. and the other Western nations. The repeated television displays of "smart" weapons scrupulously hitting strictly military targets has created the public perception that war can be waged very discretely and relatively cleanly. In fact, however, over 90% of the munitions dropped in the Gulf War were "dumb bombs" with predictable inaccuracy.

If we need to rely on such weapons in future conflicts, as will probably be the case, our opponents can propagandize the inevitable collateral damage, particularly if they widely disperse their forces among noncombatants as I imagine they will. In large measure, we will have no one to blame but ourselves because we have, as I say, oversold the salutary potential of precision munitions on modern war. Furthermore, as the U.S. and the West pour billions of scarce procurement dollars into expensive "smart" bombs in the hopes of limiting casualties, an adversary intent upon waging neo-absolutist war can rely upon cheap "dumb" munitions. Ironically, the propensity of such weapons to cause collateral damage may even serve the enemy's interests by inflicting terror on noncombatants.

In yet another manifestation of neo-absolutist war, I think that future opponents will make hostage-taking an integral part of their warmaking strategy because hostage-taking can further off-set the technological advantages of the U.S. and other First World nations. In my story, hostages are taken and chained - much as the Serbs successfully did in the Balkans - to all kinds of potential targets, including tanks, vehicles, and aircraft. The idea was to present Western forces with the terrible moral and political conundrum of having to kill civilians or even their own comrades in order to attack critical objectives. As I say, hostage-taking seems to work. I note that the Chechens successfully used hostages in several operations and I expect they will continue to do so. Nothing succeeds like success.

I also think that hostages will be taken not only from among our people, but also from the nationals of other countries. The purpose would be to pressure key nations into denying us logistical bases necessary to support forward deployed troops. In addition, since so many important communication satellites are consortium-owned, an enemy may try to use hostage-taking to blackmail member countries, including neutrals. By taking hostages from third countries, our adversary will seek to assault us employing the "indirect approach."

**Proposition #9:** Future adversaries will seek asymmetries in confronting technologically-superior opponents like the U.S. and may do so by embracing the "indirect approach."

Our future opponents, and particularly those arguably technologically weaker than the U.S., will almost certainly seek asymmetries in waging war against us and, being freed of what we would consider legal and more restraints, will look for them in places that may not be immediately apparent to us. In my article the enemy does so by applying B.H. Lidell Hart's "indirect approach," though in a somewhat different manner than perhaps he contemplated. To avoid U.S. strengths, they frequently chose to attack another, weaker country (or the nationals of that country) with a view towards influencing U.S. actions. These third countries become "proxy" or "surrogate" belligerents in a conflict in which they have few, if any, interests and are not otherwise involved. Tragically, they are attacked mainly because they could be attacked. The expectation was that their ill fortune could adversely impact the U.S. in some way.

In my fictional piece, one such "proxy" target was Mexico. The warrior-chieftain orders cyberassaults on Mexico's computer systems on the theory that they might be less well protected than those of the U.S. In addition, information-age document technologies are used to print billions in counterfeit pesos to undermine the Mexican economy. Finally, insurgency groups are encouraged to renew their activities. The collective effect of all this caused the Mexican government and economy to collapse. In turn, millions of refugees fled across the border into the United States creating a crisis there. The strategy was to divert U.S. resources and effort away from the overseas conflict while at the same time causing U.S. domestic upheaval.

I've already indicated that the nationals of minor, militarily-weak nations are used as hostages in my scenario. All of this suggests, I suppose, that one lesson of my essay might be that even in the information age small nations still need to maintain an authentic national defense capability. This capability, I submit, should include some means to project at least a deterrent force beyond its borders. Otherwise, they and their ex-patriot citizens are susceptible to becoming pawns in conflicts if for no other reason than they are vulnerable to attack. If by victimizing small, defenseless countries helps bring pressure on the U.S. or other powers, then I think that the streetfighter nations will not hesitate to do so.

But the "indirect" approach is not only applied to nations, it is aimed at domestic targets as well. If critical centers of government and business are secure against cyberassault and more conventional terror attacks, then the enemy - as was the case in my story - will seek asymmetries by striking more exposed targets. Unrestrained ethically or legally, my notional adversary chose to strike America's growing population of politically powerful elderly. Bombs were placed in parks and elder care facilities - again to divert resources and generate political difficulties.

The enemy leader in my tale engages in other, very nasty and appalling conduct. For example, he openly wages environmental war by sinking oil tankers to pollute our coasts, and scatters AIDs-infected needles on bathing beaches to create hysteria. He attacks U.S. agriculture for much the same reason that he attacked the vulnerable, "proxy" countries: because it was within his means to do so.

In each instance the warrior/streetfighter nation does not seek to hide its culpability. To the contrary, it is a precept of neo-absolutist war to use the technology-enhanced media to broadcast to the world the extreme methods that they are willing to use to achieve their ends. The enemy's fanaticism extended to sacrificing their own people in a completely unexpected way.

**Proposition #10:** Information-age warfare will likely see both new techno-weapons and more traditional arms used in innovative and unexpected ways.

One of the more startling aspects of my article was the way in which the potentate used nuclear weapons. In my story, his nation had managed to assemble a few crude nuclear devices but had no reliable way of delivering them in the face of high-tech U.S. weaponry. Accordingly, a plan was developed where an American attack is induced on the warrior-nation's "Military City" by building a genuine biological warfare lab there. The attack is carried out during a live TV news broadcast and, just as the F-117s are dropping their precision munitions, the nuclear weapon is detonated.

Of course, it appears that it was an American weapon that was detonated. There was a predictably hostile world reaction. The Japanese withdraw their support and begin to sell U.S. securities, panicking American financial markets. The rest of the world turns against the U.S., despite vehement protestations of innocence. The streetfighter nation then presents itself as a "victim state" and gains world sympathy.

I got the idea for this part of the scenario from the discussions concerning the bombing of Hiroshima and Nagasaki that took place during the World War II anniversary last year. Personally, I was amazed that the propriety of the weapons' use during that conflict was so intensely questioned and that there was - and is - so little discussion of the savagery of the Japanese aggression that was responsible for the war in the first place. This persuaded me that nuclear weapons could be used in such a way as to undermine the U.S. war effort while providing an excuse of sorts for barbaric behavior on the part of our enemy.

At the same time I wanted to suggest that although a strategy like this might be unthinkable to us, it isn't necessarily beyond the ken of other societies. Every culture does not value self-preservation above all else. We find examples throughout history - the Jews at Masada, kamikazes during World War II, the Revolutionary Guards during the Iran-Iraq War - where surely suicidal actions were more or less willingly undertaken. During the Vietnam War Buddhist monks publicly immolated themselves as a symbolic statement to advance their cause.

**Conclusions and Observations**

A fundamental lesson that I hope my nightmare scenario presents is the importance of preparing for innovative uses not only of the new information technology, but of existing weapons as well. Potential opponents may integrate both into an information-age warfighting doctrine that may be significantly different than what is popularly supposed today. Admiral Charles Turner Joy warned more than forty years ago that "we cannot expect the enemy to oblige by planning his wars to suit our weapons; we must plan our weapons to fight war where, when, and how the enemy chooses." In this regard we cannot allow our fascination with electronic gadgetry to blind us to the fact that warfighting is a holistic endeavor that has many different elements of which information technology is but one aspect, and not necessarily the most important at that.

Lest anyone misread my intentions it is my hope that by graphically discussing these issues, viable counters and defenses will be developed. That's the reason, incidentally, that the Weekly Standard piece was subtitled "a warning from the future." You may be interested to know that someone who read my article complained that I was giving potential adversaries ideas. I find it comical that anyone would think that a lawyer, sitting in his study in Papillion, Nebraska, could possibly think up strategies that our crafty potential foes overlook. In fact, I think this is another example of profoundly underestimating our likely enemies.

Such naiveté is exactly what I want to confront. As we study the implications of emerging information technologies, I urge you to evaluate these new scientific achievements from other than the Western point of view. Additionally, I recommend that you seek the views of the non-technocrat. As with anything, one's own expertise can make the forest indistinguishable from the trees. I hope that as a non-technocrat I've been able to offer some insights that are, as I like to say, "out-of-the-box."

At the conclusion of my article, I indicated that the U.S. needed to confront barbarity and cruelty promptly and unequivocally when it arises. One writer insists that the only way to deal with the emerging warrior class is to hunt them down and kill them in summary fashion. In addition to the ethical and legal problems that presents, I do not think that such a policy is practical. While I agree with the theory that warrior societies (and particularly their leaders) must suffer ignominious defeat in order to be subdued, the spectacle of summary executions presented via information-age technologies would likely sap public support for the war effort very quickly.

So I am certainly not downplaying the importance of political and diplomatic actions as some of my critics suggest. I believe, for example, that the international war crimes tribunal now sitting in the Hague is an important step towards holding accountable those who engage in barbaric behavior. I am merely saying that such behavior must be confronted in an effective way, otherwise there are too many who will perceive us as weak and see nefarious opportunity in such assumed weakness. Make no mistake about it, however, opposing savagery will often require unambiguous force of arms, to include, as Bevin Alexander predicts in The Future of War, the murderous business of soldiers physically "moving into enemy territory and taking charge." As Plato said: "Only the dead have seen the end of war."

Finally, as we consider the impact of new information-based technology on future warfare, I want to emphasize again that we must not deceive ourselves with the notion that war can somehow be made antiseptic and bloodless. This is an extremely dangerous proposition that in its worst extrapolation could even encourage conflict by deluding decision makers that the horrificness of war can be electronically avoided. As my article tried to show, even in the information age, war will remain a gory business, full of unthinkable cruelty and relentless misery. We must not forget the deadly warning of the warrior-chieftain of High-Tech War of 2007: "No computer wages war with the exquisite finality of a simple bayonet thrust." And there will always be those willing to thrust bayonets to achieve their aims.